AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter.

1. (Currently Amended) A method for over-the-air (OTA) activation of a wireless unit in a particular communications system, comprising the steps of:

A. causing the wireless unit to include a stored key, the stored key having been generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm.

B. causing the wireless unit to receive ~~the~~ a wireless unit parameter[s] and a verification number over-the-air, the wireless unit parameter[s] including an identification of the particular communications system,

i. the verification number having been generated by using an authorization algorithm (A-algorithm) having the wireless unit parameter[s] and a key as A-algorithm inputs, and

ii. the key having been generated by the K-algorithm having the identifier associated with the wireless unit as the K-algorithm input;

C. in response to receipt of the wireless unit parameter[s] and the verification number, causing the wireless unit to generate a trial verification number by using the A-algorithm with the wireless unit parameter[s] and the stored key as trial inputs;

D. causing the wireless unit to compare the verification number to the trial verification number for a match; and

E. in response to finding the match, causing the wireless unit to use the wireless unit parameter[s] for activation of the wireless unit in the particular communications system.

2. (Currently Amended) The method of Claim 1, further ~~comprising~~ including the step of:

F. in response to failing to find the match, causing the wireless unit to fail to use the wireless unit parameter[s] for the activation of the wireless unit in the particular communications system.

3. (Currently Amended) The method of Claim 1, wherein the wireless unit parameter[s] comprises numeric assignment module (NAM) parameters.

4. (Original) The method of Claim 1, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

5. (Currently Amended) A method to prevent a wireless unit from being programmed over-the-air (OTA), comprising the steps of:

A. causing the wireless unit to include a stored key, the stored key being generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm;

B. causing the wireless unit, in response to receipt of information transmitted OTA to the wireless unit, to generate a trial verification number by using an authorization algorithm (A-algorithm) with the stored key and the information as A-algorithm inputs to the A-algorithm;

C. causing the wireless unit to compare the trial verification number with at least a portion of the information for a match; and

D. causing the wireless unit, in response to failing to find the match, to block programming of the wireless unit.

6. (Original) The method of Claim 5, wherein the information transmitted OTA to the wireless unit comprises numeric assignment module (NAM) parameters.

7. (Original) The method of Claim 5, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

8. (Original) The method of Claim 5, wherein the programming of the wireless unit comprises activation of the wireless unit in a particular communications systems; and wherein causing the wireless unit to block the programming of the wireless unit comprises causing the wireless unit to block the activation of the wireless unit in the particular communications system.

9. (Currently Amended) A method for secure over-the-air (OTA) programming of a wireless unit, comprising the steps of:

A. causing the wireless unit to include a stored key;

B. causing the wireless unit to receive OTA wireless unit parameter[s] and a verification number;

C. in response to receipt of the wireless unit parameter[s] and the verification number, causing the wireless unit to generate a trial verification number;

D. causing the wireless unit to compare the verification number to the trial verification number for a match; and

E. in response to finding the match, causing the wireless unit to use the wireless unit parameter[s] for programming of the wireless unit.

10. (Currently Amended) The method of Claim 9, further ~~comprising~~ including the step of:

F. in response to failing to find the match, causing the wireless unit to block the programming of the wireless unit.

11. (Currently Amended) The method of Claim 9, wherein ~~action A comprises~~ step A further includes the step of:

causing the wireless unit to include the stored key, the stored key having been generated by using a key algorithm (K-algorithm) and having an identifier associated with the wireless unit as a K-algorithm input.

12. (Original) The method of Claim 11, wherein the identifier associated with the wireless unit comprises an electronic serial number (ESN) of the wireless unit.

13. (Original) The method of Claim 9, wherein the stored key is relatively unique to the wireless unit.

14. (Currently Amended) The method of Claim 9, wherein ~~action B comprises~~ step B further includes the step of:

causing the wireless unit to receive OTA the wireless unit parameter[s] and the verification number, the verification number having been generated by an authorization algorithm (A-algorithm) having the wireless unit parameter[s] and a key as A-algorithm inputs.

15. (Original) The method of Claim 14, wherein the key has been generated by a key algorithm (K-algorithm) having an identifier associated with the wireless unit as a K-algorithm input.

16. (Original) The method of Claim 14, wherein the key is relatively unique to the wireless unit.

17. (Currently Amended) The method of Claim 9, wherein step C further includes the step of: ~~action C comprises,~~

in response to receipt of the wireless unit parameter[s] and the verification number, causing the wireless unit to generate the trial verification number by using the wireless unit parameter[s] and the stored key.

18. (Currently Amended) The method of Claim 17, wherein step C further includes the step of: ~~action C comprises,~~

in response to receipt of the wireless unit parameter[s] and the verification number, causing the wireless unit to generate the trial verification number by using an authorization algorithm (A-algorithm) with the wireless unit parameter[s] and the stored key as A-algorithm inputs.

19. (Currently Amended) The method of Claim 9, wherein the wireless unit parameter[s] comprises numeric assignment module (NAM) parameters.

20. (Currently Amended) The method of Claim 9, wherein the programming of the wireless unit comprises activation of the wireless unit in a particular communications system; and wherein causing the wireless unit to use the wireless unit parameter[s] for the programming of the wireless unit comprises causing the wireless unit to activate the wireless unit in the particular communications system.

21. (Original) A wireless unit that can be programmed over-the-air (OTA) by only a particular service provider, the wireless unit comprising:

a memory for storing a stored key relatively unique to the wireless unit and for storing wireless unit information;

a control for receipt of information OTA from the particular service provider;

a processor being functionally connected to the control and to the memory, and for, in response to the receipt of the information OTA from the particular service provider,

effecting generation of a trial verification number,

effecting comparison of the trial verification number with at least a portion of the information from the particular service provider for a match, and

in response to finding the match, effecting the storing of the information in the memory,

whereby the wireless unit can be programmed OTA only by the particular service provider that provides the information that results in the match with the trial verification number.

22. (Original) The wireless unit of Claim 21, wherein the stored key is generated by using a key algorithm (K-algorithm) with an identifier associated with the wireless unit as an input to the K-algorithm.

23. (Original) The wireless unit of Claim 22, wherein the identifier comprises an electronic serial number (ESN) of the wireless unit.

24. (Original) The wireless unit of Claim 22, wherein the stored key is generated by the wireless unit using the K-algorithm with the identifier associated with the wireless unit as the input to the K-algorithm.

25. (Original) The wireless unit of Claim 21, wherein the information comprises numeric assignment module (NAM) parameters.

26. (Original) The wireless unit of Claim 25, wherein the information comprises the NAM parameters and a verification number; and wherein the processor is operative to effect a comparison between the trial verification number and the verification number for the match.

27. (Original) The wireless unit of Claim 26, wherein the verification number is generated by an authorization algorithm (A-algorithm) having the NAM parameters and a key as A-algorithm inputs.

28. (Original) The wireless unit of Claim 27, wherein the key is generated by a key algorithm (K-algorithm) having an electronic serial number (ESN) associated with the wireless unit as a K-algorithm input.

29. (Original) The wireless unit of Claim 21, wherein the trial verification number is generated by using an authorization algorithm (A-algorithm) with the NAM parameters and the stored key as A-algorithm inputs.

30. (Original) The wireless unit of Claim 21, wherein the processor is operative, in response to failing to find the match, to block the storing of the information.

31. (Original) The wireless unit of Claim 21, wherein the programming comprises activation of the wireless unit in a particular communications system.

32. (New) A unit that is locked against use for communications until the unit is unlocked, comprising:

memory for storing an unlock code with the unlock code being generated from an algorithm using a secret code and an identifier of the unit;

a control for receipt of an input code; and

a processor being functionally connected to the control and to the memory to effect a comparison of the input code to the unlock code, and to effect an unlocking of the unit if the comparison results in a finding that the input code is substantially equal to the unlock code.

33. (New) The unit of Claim 32, wherein the identifier comprises an identifier unique to the unit.

34. (New) The unit of Claim 32, wherein the identifier comprises an electronic serial number of the unit.

35. (New) The unit of Claim 32, wherein the control is operative to receive the input code and a system identification number from a selected network; and wherein the processor is operative, after the unlocking of the unit, to effect activation of the unit on the selected network based on the system identification number.

36. (New) The unit of Claim 32, wherein the algorithm comprises a cryptographic algorithm; and wherein the unlock code comprises a pseudo-random output generated by the cryptographic algorithm.

37. (New) The unit of Claim 32, wherein the algorithm comprises a cave algorithm; and wherein the unlock code comprises a subset of mixing register result generated by the cave algorithm.

38. (New) The unit of Claim 32, wherein the algorithm comprises an MD5 algorithm; and wherein the unlock code comprises a subset of an MD5 result.

39. (New) The unit of Claim 32, wherein the algorithm used to generate the unlock code is run by a device other than the unit; and

wherein the unlock code is loaded by the device in the memory.

40. (New) The unit of Claim 32, wherein the unit comprises a wireless unit; and wherein the identifier comprises an electronic serial number of the wireless unit.

41. (New) The unit of Claim 32, wherein the algorithm includes division of a secret code by an identifier of the unit.

42. The unit of Claim 41, wherein the division of the secret code by the identifier of the unit results in a remainder and the remainder is the secret code.

43. (New) With respect to a unit loaded with an identifier, a method to render the unit useless for communications until the unit is unlocked, the method comprising the steps of:

generating an unlock code by using an algorithm with

a secret code and the identifier;

storing the unlock code in the unit; and

configuring the unit to be unlocked through input into the unit of an input code substantially equal to the unlock code,

whereby the unit cannot be used for communications until the unit is unlocked with the input of the input code substantially equal to the unlock code.

44. (New) The method of Claim 43, wherein generating the unlock code comprises causing the unit to generate the unlock code by using the algorithm to divide the secret code by the identifier.

45. (New) The method of Claim 44, wherein dividing the secret code by the identifier produces a remainder, and further including the step of selecting the remainder as the unlock code.

46. (New) The method of Claim 43, wherein the algorithm comprises a cave algorithm; and wherein generating the unlock code comprises using the cave algorithm.

47. (New) The method of Claim 43, wherein the algorithm comprises an MD5 algorithm; and wherein generating the unlock code comprises using the MD5 algorithm.

48. (New) The method of Claim 43, further comprising:
receiving a system identification number from a selected network; and
based on unlocking of the unit, activating the unit on the selected network.

49. (New) With respect to a unit that has been loaded with an identifier and that has been locked, a method to unlock the unit for communications, comprising the steps of:
generating an unlock code using an algorithm with a secret code and an identifier;
receiving an input code;
comparing the input code to the unlock code; and
unlocking the unit if the input code is substantially equal to the unlock code.

50. (New) The method of Claim 49, wherein generating the unlock code comprises causing the unit to generate the unlock code by using the algorithm to divide

the secret code by the identifier. to obtain a remainder, and to select the remainder as the unlock code.

51. (New) The method of Claim 49, wherein dividing the secret code by the identifier produces a remainder, and further including the step of selecting the remainder as the unlock code.

52. (New) The method of Claim 49, further including the steps of:

receiving a system identification number from a selected network; and

based on the unlocking of the unit, activating the unit on the selected network.

53. (New) The method of Claim 49, wherein receiving the input code comprises receiving the input code from a selected network; and further including the steps of:

receiving a system identification number from the selected network; and

based on the unlocking of the unit, activating the unit on the selected network.

54. (New) The method of Claim 49, wherein generating the unlock code comprises causing the unlock code to be generated by a device other than the unit.

55. (New) A computer-readable medium on which is stored a computer program for rendering a unit useless for operation until the unit is unlocked, the unit having an identifier unique to the unit, the computer program comprising instructions, which when executed by a computer perform the steps of:

obtaining a secret code;

using the secret code with the identifier in an algorithm to generate an unlock code;

loading the unit with the unlock code; and

configuring the unit so that the unit can only be unlocked through input into the unit of an input code substantially equal to the unlock code.

56. (New) The computer-readable medium of Claim 55, wherein the algorithm comprises a cave algorithm; and wherein using the secret code with the identifier in the algorithm to generate the unlock code comprises using the secret code with the identifier in the cave algorithm to generate the unlock code.

57. (New) The computer-readable medium of Claim 55, wherein the algorithm comprises an MD5 algorithm; and wherein using the secret code with the identifier in the algorithm to generate the unlock code comprises using the secret code with the identifier in the MD5 algorithm to generate the unlock code.

58. (New) The computer-readable medium of Claim 55, wherein the algorithm comprises division of the secret code by the identifier of the unit.

59. (New) The computer-readable medium of Claim 58, wherein the division of the secret code by the identifier of the unit results in a remainder and the remainder is the secret code.

60. (New) A method of controlling use of a communications unit having an identifier, the method comprising the steps of:

configuring the communication unit to be lockable;

configuring the communication unit to be unlockable; and

generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

61. (New) The method of claim 60, wherein the step of generating further includes the step of:

using an algorithm and a secret code in conjunction with the identifier.

62. (New) The method of claim 61, wherein the algorithm is a cryptographic function.

63. (New) The method of claim 62, wherein the cryptographic function is a hash function.

64. (New) The method of claim 62, wherein the cryptographic function is a checksum function.

65. (New) The method of claim 60, wherein the step of generating further includes the step of:

using a secret code and at least the identifier in a mathematical operation to generate the unlock code.

66. (New) The method of claim 65, wherein the mathematical operation is division, and the secret code is divided by the identifier.

67. (New) The method of claim 66, wherein the secret code is related to the remainder.

68. (New) The method of claim 67, wherein the remainder is padded, and the padded remainder is the secret code.

69. (New) The method of claim 67, wherein the remainder is the secret code.

70. (New) The method of claim 67, wherein the communication unit cannot be used for communications responsive to the communication unit being in a locked state.

71. (New) The method of claim 67, wherein the communication unit can be used for communications responsive to the communication unit being in an unlocked state.

72. (New) A lockable/unlockable communication unit, the communication unit comprising:

a memory having unlock code stored therein, the unlock code generated using at least the identifier;

a control adapted to receive a input code; and

a processor in communication with the control and the memory, the processor adapted to compare the unlock code with the input, and responsive to the input being substantially equal to the unlock code, the processor effects a change of state from locked to unlocked.

73. (New) The unit of claim 72, wherein the identifier comprises an identifier

unique to the unit.

74. (New) The unit of claim 72, wherein the identifier comprises an electronic serial number of the unit.

75. (New) The unit of claim 72, wherein the communication unit is unable to communicate when the communication unit is in a locked state.

76. (New) A system for controlling use of a communication unit, the system comprising:

means for configuring the communication unit to be lockable;

means for configuring the communication unit to be unlockable; and

means for generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

77. (New) The system of claim 76, wherein the means for generating the unlock code uses an algorithm and a secret code in conjunction with the identifier.

78. (New) The system of claim 77, wherein the algorithm is a cryptographic function.

79. (New) The system of claim 78, wherein the cryptographic function is a hash function.

80. (New) The system of claim 78, wherein the cryptographic function is a checksum function.

81. (New) The system of claim 76, wherein the means for generating the unlock code uses a secret code and at least the identifier in a mathematical operation to generate the unlock code.

82. (New) The system of claim 81, wherein the mathematical operation is division, and the secret code is divided by the identifier.

83. (New) The system of claim 82, wherein the secret code is related to the remainder.

84. (New) The system of claim 83, wherein the remainder is padded, and the padded remainder is the secret code.

85. (New) The system of claim 83, wherein the remainder is the secret code.

86. (New) The system of claim 76, wherein the communication unit cannot be used for communications responsive to the communication unit being in a locked state.

87. (New) The system of claim 76, wherein the communication unit can be used for communications responsive to the communication unit being in an unlocked state.

88. (New) A computer-readable medium on which is stored a computer program for controlling use of a communication unit having an identifier, the computer program comprising instructions, which when executed by a computer perform the steps of:

configuring the communication unit to be lockable;

configuring the communication unit to be unlockable; and

generating an unlock code for the communication unit using at least the identifier, wherein the unlock code is used to change the state of the communication unit from locked to unlocked.

89. (New) The computer-readable medium of Claim 88, wherein the step of generating further includes the step of:

using an algorithm and a secret code in conjunction with the identifier.

90. (New) The computer-readable medium of claim 89, wherein the algorithm is a cryptographic function.

91. (New) The computer-readable medium of claim 90, wherein the cryptographic function is a hash function.

92. (New) The computer-readable medium of claim 90, wherein the cryptographic function is a checksum function.

93. (New) The computer-readable medium of claim 88, wherein the step of generating further includes the step of:

using a secret code and at least the identifier in a mathematical operation to generate the unlock code.

94. (New) The computer-readable medium of claim 93, wherein the mathematical operation is division, and the secret code is divided by the identifier.

95. (New) The computer-readable medium of claim 94, wherein the secret code is related to the remainder.

96. (New) The computer-readable medium of claim 95, wherein the remainder is padded, and the padded remainder is the secret code.

97. (New) The computer-readable medium of claim 95, wherein the remainder is the secret code.